Algebraic properties of polar codes from a new polynomial formalism

Magali Bardet, Vlad Dragoi, Ayoub Otmani, Jean-Pierre Tillich

▶ **To cite this version:**

Magali Bardet, Vlad Dragoi, Ayoub Otmani, Jean-Pierre Tillich. Algebraic properties of polar codes from a new polynomial formalism. International Symposium on Information Theory ISIT 2016, Jul 2016, Barcelona, Spain. pp.230 - 234, 10.1109/ISIT.2016.7541295 . hal-01410210

HAL Id: hal-01410210
https://inria.hal.science/hal-01410210

Submitted on 6 Dec 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Algebraic Properties of Polar Codes From a New Polynomial Formalism

Magali Bardet*, Vlad Dragoi*, Ayoub Otmani*, Jean-Pierre Tillich†
*Normandie Univ, France; UR, LITIS, F-76821 Mont-Saint-Aignan, France
{magali.bardet,vlad.dragoi1,ayoub.otmani}@univ-rouen.fr
†Inria, SECRET Project, 78153 Le Chesnay Cedex, France
{jean-pierre.tillich}@inria.fr

***Abstract*—Polar codes form a very powerful family of codes with a low complexity decoding algorithm that attains many information theoretic limits in error correction and source coding. These codes are closely related to Reed-Muller codes because both can be described with the same algebraic formalism, namely they are generated by evaluations of monomials. However, finding the right set of generating monomials for a polar code which optimises the decoding performances is a nontrivial task and is channel dependent. The purpose of this paper is to reveal some universal properties of these monomials. We will namely prove that there is a way to define a nontrivial (partial) order on monomials so that the monomials generating a polar code devised for a binary-input symmetric channel always form a decreasing set. We call such codes decreasing monomial codes. The fact that polar codes are decreasing monomial codes turns out to have rather deep consequences on their structure. Indeed, we show that decreasing monomial codes have a very large permutation group by proving that it contains a group called lower triangular affine group. Furthermore, the codewords of minimum weight correspond exactly to the orbits of the minimum weight codewords that are obtained from evaluations of monomials of the generating set. In particular, it gives an efficient way of counting the number of minimum weight codewords of a decreasing monomial code and henceforth of a polar code.**

I. Introduction

Polar codes and Reed Muller codes viewed as monomial codes. Polar codes were discovered by Arıkan [1] and form a very powerful family of codes that gave a nice constructive way of attaining many information theoretic limits in error correction and source coding. In particular, they allow to attain the capacity of any symmetric memoryless channel with a low complexity decoding algorithm (namely the successive cancellation decoder of Arıkan). These codes are closely related to Reed-Muller codes in the sense that they can both be described with the same algebraic formalism, namely as *monomial* codes. Monomial codes are evaluation codes where a specific set of monomials provides a generator matrix. A Reed-Muller code $\mathscr{R}(r,m)$ is generated by the evaluation over $\mathbb{F}_2^m$ of *all* monomials degree at most r in m variables. A polar code of length 2^m is also generated by evaluation of monomials, but not necessarily by the same monomials as a Reed-Muller code: if we want a polar code of a certain dimension for a certain channel, we are going to take a very specific set of monomials which is in general significantly different from the Reed-Muller choice. This choice will give good performances for the Arıkan successive cancellation decoder. It turns out that this decoder is very closely related to Dumer's recursive algorithm for decoding Reed-Muller codes [2] based on the $(u|u+v)$ decomposition. Basically Dumer's decoding algorithm is the successive cancellation decoder of Arıkan but the performance of the decoder is much worse in this case because the choice of monomials for a Reed-Muller code is not well suited to this kind of decoding algorithm.

Polar codes are decreasing monomial codes. Finding the right set of generating monomials for a polar code which optimises the decoding performances under the successive cancellation decoder is by no means an easy task (see for instance [3]) and moreover it is channel dependent. Our purpose is here to reveal some universal properties of these monomials, where by "universal" we mean properties that do not depend on the channel. We will namely prove that, regardless of the binary-input symmetric channel the polar code is devised for, there is a way to define a nontrivial partial order on monomials for which a polar code is always generated by a *decreasing set*, that is to say: if a monomial lies in the generating set then all monomials that are smaller also belong to it. This property turns out to have rather deep consequences on the structure of the polar code. We call *decreasing monomial code* a monomial code whose generating set of monomials forms a decreasing set. We will namely prove that such codes have some interesting properties.

The permutation group of decreasing monomial codes. The *permutation group* of a code is the group of the permutations of coordinates leaving the code globally invariant, *i.e.* it permutes the coordinates of any codeword into another codeword. It is well known that the permutation group of a non-trivial Reed-Muller code $\mathscr{R}(r,m)$ is isomorphic the whole affine group $\mathbb{A}_m$ over $\mathbb{F}_2^m$. This group is of size $2^{\Theta(m^2)}$ which is superpolynomial in the length $n=2^m$ of the Reed-Muller code, since it is of size $n^{\Theta(\log n)}$. It is also 2-transitive and this property has been used recently to prove that Reed-Muller codes attain the capacity of the erasure channel [4], [5]. The fact that the size of the permutation group of a Reed-Muller code $\mathscr{R}(r,m)$ is so large is related to the special choice of generating monomials of the code: the affine group actually acts in a natural way on monomials and transforms a monomial in the generating set into a sum of monomials of the generating set, since by an affine change of variables a monomial of degree less than or equal to r is transformed into a polynomial

of degree less than or equal to r.

We do not expect such a behavior for polar codes, since the monomial generating set of the polar code has no reason to have the same property. However it will turn out that because of the fact that the set of monomials of the polar code is decreasing with our order this set of monomials is transformed by the lower triangular affine group (corresponding to affine transformations $\boldsymbol{x} \mapsto \boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}$ where $\boldsymbol{A}$ is a lower triangular matrix with 1's on its diagonal) into a sum of monomials that still belong to the generating set. This will imply that the permutation group of a polar code, and of a decreasing monomial code in general, contains a subgroup which is isomorphic to the lower triangular affine group. For a decreasing monomial code of length 2^m this subgroup is also of size $2^{\Theta(m^2)}$ which is also superpolynomial in the length $n = 2^m$ of the code. In other words, in a rather unexpected way, as in the case of Reed-Muller code the permutation group of a polar code is also extremely large (although it may only be one-transitive in this case).

The structure of codewords of minimum weight in a decreasing monomial code. The fact that the permutation group of a decreasing monomial code, and of a polar code in particular, is so large can be used for a better understanding of the structure of such codes. In particular we might expect to classify such codes as it has been done for affine invariant codes [6]. Here we are going to use it to give a very convenient description of the minimal codewords. Indeed, a codeword of minimum weight is transformed into another minimal codeword by the action of the permutation group of the code. It turns out that this number of orbits is very small, since we are going to show that any such orbit contains a generating monomial of maximum degree. Therefore the number of such orbits is really small since it is at most of size $O(n)$ where n is the length of the code. Moreover it is also rather easy to count the number of elements in the orbit and this will allow to count the number of codewords of minimum weight.

Due to space constraints, all the proofs have been omitted. The full version of this paper can be found on the `arXiv.org` preprint server.

II. Reed-Muller, Monomial and Polar Codes

In this section we briefly review Reed-Muller codes, polar codes and the algebraic formalism we will use to describe both families.

Reed-Muller codes. It is well known that Reed-Muller codes of length 2^m can be obtained as evaluation codes of polynomials in $\mathbb{F}_2[x_0, \dots, x_{m-1}]$. Polar codes can also be described through this formalism. Since we are interested in evaluations of such polynomials over entries in $\mathbb{F}_2^m$ we will identify x_i with x_i^2 and work in the ring $\mathbf{R}_m = \mathbb{F}_2[x_0, \dots, x_{m-1}]/(x_0^2 - x_0, \dots, x_{m-1}^2 - x_{m-1})$. It will be convenient with this formalism to associate to a polynomial $g \in \mathbf{R}_m$ the binary vector denoted by $\mathsf{ev}(g)$ in $\mathbb{F}_2^n$ with $n = 2^m$ which is the evaluation of the polynomial in all the binary entries $\boldsymbol{u} = (u_0, \dots, u_{m-1}) \in \mathbb{F}_2^m$. In other words

$$\mathsf{ev}(g) = \big(g(\boldsymbol{u})\big)_{\boldsymbol{u} \in \mathbb{F}_2^m}$$

With this notation, we view the indices as elements of $\mathbb{F}_2^m$. This notation does not specify the order we use for the elements of $\mathbb{F}_2^m$. We actually use the natural order by viewing $\boldsymbol{u} = (u_0, \dots, u_m)$ as the integer $\sum_{i=0}^{m-1} u_i 2^i$ where $u_i \in \{0, 1\}$. With this notation at hand, the Reed-Muller code $\mathscr{R}(r, m)$ is defined as

$$\mathscr{R}(r, m) \stackrel{\text{def}}{=} \big\{\mathsf{ev}(P) \mid P \in \mathbf{R}_m, \deg P \leqslant r\big\}$$

The function $\mathsf{ev} : \mathbf{R}_m \to \mathbb{F}_2^n$ is an homomorphism of algebra. Hence, the code $\mathscr{R}(r, m)$ is generated by the codewords $\mathsf{ev}(g)$ where g is a monomial of degree less than or equal to r. Recall that a *monomial* is any product of variables of the form $x_0^{g_0} \cdots x_{m-1}^{g_{m-1}}$ where $g_0, \dots, g_{m-1}$ are binary. The set of all monomials is denoted by:

$$\mathcal{M}_m \stackrel{\text{def}}{=} \left\{x_0^{g_0} \cdots x_{m-1}^{g_{m-1}} \mid (g_0, \dots, g_{m-1}) \in \mathbb{F}_2^m\right\}.$$

Reed-Muller codes have a very large permutation group which is isomorphic to the affine group over $\mathbb{F}_2^m$.

Monomial codes. Monomial codes form a very general family of codes that generalizes Reed-Muller codes.

Definition 1 (Monomial code)**.** *Let $I \subseteq \mathcal{M}_m$ be a finite set of monomials in m variables and set $n \stackrel{def}{=} 2^m$. The linear code defined by I is the vector subspace $\mathscr{C}(I) \subseteq \mathbb{F}_2^n$ generated by $\{\mathsf{ev}(f) \mid f \in I\}$.*

The dimension of such codes is given by

Proposition 1. *For all $I \subseteq \mathcal{M}_m$ the dimension of the monomial code $\mathscr{C}(I)$ is equal to $|I|$.*

Proof: This comes from the linear independence of the monomials in $\mathbf{R}_m$ and the fact that ev is an injective mapping from $\mathbf{R}_m$ to $\mathbb{F}_2^{2^m}$. ∎

Polar codes. What we call here a polar code is a binary polar code as defined by Arıkan in [1]. They can be described as codes of length $n = 2^m$, where m is an arbitrary integer. They may take any dimension between 1 and 2^m. The polar code of length $n = 2^m$ and dimension k is obtained through a generator matrix which picks a specific subset of k rows of the $2^m \times 2^m$ matrix:

$$\boldsymbol{G}_m \stackrel{\text{def}}{=} \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{m \text{ times}}.$$

Note that we depart here slightly from the usual convention for polar codes which is to use in the Kronecker product the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. The two definitions (ours and the standard one) are easily seen to be equivalent, they just amount to order the code positions differently. Our convention presents the advantage of simplifying the polynomial formalism that follows. It is clear that a polar code is a monomial code. This comes from the fact

that the rows of $\boldsymbol{G}_m$ are all possible evaluations of monomials. This fact is proved by induction on m by observing that $(1,1)$ is the evaluation over $\mathbb{F}_2$ of the constant monomial 1 and that $(0,1)$ is the evaluation over $\mathbb{F}_2$ of the monomial x_0. If we consider the binary expansion of each row number (starting from 0 to 2^m-1) of $\boldsymbol{G}_m$ over m bits $i=\sum_{j=0}^{m-1} i_j 2^j$ (where $i_j \in \{0,1\}$), then the row of index i of $\boldsymbol{G}_m$ is given by $\boldsymbol{G}_m[i] = \mathsf{ev}(x_0^{i_0}\dots x_{m-1}^{i_{m-1}})$.

In essence, constructing a polar code of dimension k is equivalent to finding the k "best" bit-channels that modelize the channel that the decoder sees when it recovers one by one the information bits corresponding to the received codeword by the successive cancellation decoder. We refer to [1] for the definition of the successive decoder and just give here the decision rule for choosing the generating monomial of the polar code viewed as a monomial code. For this purpose denote by W the memoryless channel for which the polar code is devised. Its input alphabet is binary and its output alphabet is denoted by $\mathcal{Y}$ and for the sake of simplifying a little bit the discussion, it is also assumed to be discrete. We assume that the channel is symmetric meaning that there exists a permutation π of $\mathcal{Y}$ which is also an involution ($\pi^{-1}=\pi$) and $W(y|1) = W(\pi(y)|0)$ for all $y \in \mathcal{Y}$. We define the Arıkan channel transforms W^+ and W^- of W which are both binary-input memoryless symmetric channel with transitions probabilities specified by

$$\begin{aligned} W^+(y_1,y_2,u_2|u_1) &\stackrel{\text{def}}{=} \frac{1}{2}W(y_1|u_1)W(y_2|u_1\oplus u_2) \\ W^-(y_1,y_2|u_2) &\stackrel{\text{def}}{=} \frac{1}{2}\sum_{u_1\in\mathbb{F}_2} W(y_1|u_1)W(y_2|u_1\oplus u_2) \end{aligned}$$

Here the output alphabet of W^- is $\mathcal{Y}\times\mathcal{Y}$ whereas the output alphabet of W^+ is $\mathcal{Y}\times\mathcal{Y}\times\mathbb{F}_2$. Finally we will also need to define the Bhattacharyya parameter $\mathcal{B}(W)$ of a binary-input symmetric channel W. It is given by

$$\mathcal{B}(W) \stackrel{\text{def}}{=} \sum_{y\in\mathcal{Y}} \sqrt{W(y|0)W(y|1)}$$

With these definitions we can construct a polar code of length $n=2^m$ and dimension k devised for a binary-input symmetric channel W.

Definition 2. *The polar code of length $n=2^m$ and dimension k devised for the channel W is the monomial code $\mathscr{C}(I)$ where I is the set of k monomials in $\mathcal{M}_m$ which take the k smallest values $\mathcal{B}(W^g)$ among all g in $\mathcal{M}_m$.*

Note that the output alphabet size of the channels W^g is exponential in m which makes this ranking rather delicate. However there are efficient methods for computing these k "best" channels, see for instance [3] where ranking is performed for the error probability which is arguably even more complicated to track than the Bhattacharyya parameter.

III. Decreasing Monomial Codes

Polar codes and Reed-Muller codes are both monomial codes but this family is too large to explain the intriguing algebraic properties of polar codes (for instance their very large automorphism group). We also want to capture simple properties that give some insight about which monomials to choose in a polar code and this for any channel. Of course, W^+ is a much better channel than W^- and it is straightforward to prove based on this intuition that a polar code of nonzero dimension always involves the monomial 1 in its definition and this for every channel. We will prove guided by this "principle" that if f divides g and if g is a monomial in the defining monomial set I of the polar code $\mathscr{C}(I)$ then f also belongs to I. If we define the partial order between monomials induced by divisibility considerations, that is $f \preceq_{\text{w}} g$ iff f divides g, then the defining monomial set I of a polar code $C(I)$ is *decreasing*, meaning that if $g\in I$ any f such that $f\preceq_{\text{w}} g$ also belongs to I. Here the "w" in $\preceq_{\text{w}}$ stands for "weak" (as in weak order) to distinguish between this divisibility partial order and a much finer order that we will introduce below.

This divisibility order was already used by Mori and Tanaka in order to tighten up the bounds for the block error probability of the SC decoder for Polar codes over the BEC (see Section VI,[7]). It also can be used to prove that the permutation group of a polar code contains a group isomorphic to $\mathbb{Z}_2^m$ for a polar code of length 2^m. This proves that polar codes admit a 1-transitive permutation group for instance. But we can go much beyond this by introducing a much finer ordering of the monomials than the divisibility ordering $\preceq_{\text{w}}$ which can eventually might be used to tighten even more the results in [7]. The order we will consider is the following

Definition 3. *Two monomials of the same degree are ordered as $x_{i_1}\dots x_{i_s} \preceq x_{j_1}\dots x_{j_s}$ if and only if for any $\ell\in\{1,\dots,s\}$, it holds $i_\ell \leqslant j_\ell$ where we assume $i_1<\dots<i_s$ and $j_1<\dots<j_s$.*

This partial order is extended to monomials of different degrees through divisibility, namely $f\preceq g$ if and only if there is a divisor g^* of g such that $f\preceq g^*\preceq_w g$.

From this definition, for any monomial f of $\mathcal{M}_m$ the constant polynomial 1 satisfies the inequality $1\preceq f$. We also have that $x_0\preceq x_1\preceq\dots\preceq x_{m-1}$. The *interval* $[f,h]$ where f and h are in $\mathcal{M}_m$ with $f\preceq h$ is the set of monomials $g\in\mathcal{M}_m$ such that $f\preceq g\preceq h$. We will also need the following definition

Definition 4. *A set $I\subseteq\mathcal{M}_m$ is* decreasing *if and only if ($f\in I$ and $g\preceq f$) implies $g\in I$. A set $I\subseteq\mathcal{M}_m$ is* weakly decreasing *if and only if ($f\in I$ and $g\preceq_w f$) implies $g\in I$.*

When $I\subseteq\mathcal{M}_m$ is a decreasing *set then $\mathscr{C}(I)$ is called* decreasing monomial code*. It is called a* weakly decreasing monomial code *if I is weakly decreasing.*

Reed-Muller codes are decreasing codes because :

$$\mathscr{R}(r,m) = \mathscr{C}\left([1, x_{m-r}\cdots x_{m-1}]\right). \tag{1}$$

. It will turn out that polar codes devised for any binary-input symmetric channel are decreasing monomial codes.

Theorem 1. *Polar codes are decreasing monomial codes.*

IV. Structural Properties of Decreasing Monomial Codes

The algebraic formalism introduced in previous sections permits to reveal several interesting properties about decreasing monomial codes. In this section, we focus only on three important aspects: characterising the dual code, estimating the minimum distance and identifying a large subgroup of the permutation group.

A. Duality

It is readily seen that the dual of a monomial code is a polynomial code, but it is not necessarily a monomial code. However the dual of a decreasing monomial code turns out to be a decreasing monomial code. In order to describe precisely the duality we will define some notation.

The set of indexes of the variables appearing in a monomial $g \in \mathcal{M}_m$ is denoted by $\mathrm{ind}(g)$. Hence, we have $g = \prod_{i \in \mathrm{ind}(g)} x_i$. The *multiplicative complement* of a monomial $g \in \mathcal{M}_m$ denoted by $\check{g}$, is defined as: $\check{g} = \prod_{i \in \{0,\dots,m-1\} \setminus \mathrm{ind}(g)} x_i$ By extension for any subset $I \subseteq \mathcal{M}_m$, the set $\check{I} \subseteq \mathcal{M}_m$ denotes $\{\check{f} \ : \ f \in I\}$.

Proposition 2. *Let $\mathscr{C}(I)$ be a decreasing monomial code, then its dual is a decreasing monomial code given by*

$$\mathscr{C}(I)^{\perp} = \mathscr{C}(\mathcal{M}_m \setminus \check{I}).$$

A straightforward consequence of this is that under some conditions, any decreasing monomial code is weakly self-dual.

Corollary 1. *Let $\mathscr{C}(I)$ be a decreasing monomial code with $|I| \leqslant \frac{1}{2}2^m$. Then $\mathscr{C}(I) \subseteq \mathscr{C}(I)^{\perp}$ if and only if for any $f \in I,\ \check{f} \notin I$.*

Polar codes of rate (sufficiently) smaller than $1/2$ generally satisfy this assumption and in the case of rate greater than $\frac{1}{2}$ it is the dual of the polar code that satisfies this assumption. This can be explained by looking at the polarization process that is used to choose the monomials defining the polar code.

B. Minimum Distance of Decreasing Monomial Codes

The minimum distance of both Reed-Muller [8] and Polar codes [9] is already known. Nevertheless for our algebraic formalism it will be convenient to introduce a different notation.

Definition 5. *Let $\mathscr{C}(I)$ be a decreasing monomial code over m variables. We let*

$$\begin{aligned} r_-(\mathscr{C}(I)) &\stackrel{def}{=} \max\left\{r \mid \mathscr{R}(r,m) \subseteq \mathscr{C}(I)\right\} \\ r_+(\mathscr{C}(I)) &\stackrel{def}{=} \min\left\{r \mid \mathscr{C}(I) \subseteq \mathscr{R}(r,m)\right\} \end{aligned}$$

It is readily checked that another way of defining these quantities is that r_- is the largest r for which the monomial $x_{m-r}\cdots x_{m-1}$ is in I. On the other hand r_+ is the largest integer r for which $x_0 \cdots x_{r-1}$ is in I. These quantities are related to the minimum distance of a decreasing monomial code and its dual through the following result

Proposition 3. *Let $\mathscr{C}(I)$ be a decreasing monomial code over m variables. We have the following properties:*

1) *The minimum distance of $\mathscr{C}(I)$ is equal to $2^{m-r_+(\mathscr{C}(I))}$.*
2) *$r_-(\mathscr{C}(I)^{\perp})$ and $r_+(\mathscr{C}(I)^{\perp})$ satisfy the equalities:*

$$\begin{aligned} r_-(\mathscr{C}(I)^{\perp}) &= m - 1 - r_+(\mathscr{C}(I)) \\ r_+(\mathscr{C}(I)^{\perp}) &= m - 1 - r_-(\mathscr{C}(I)) \end{aligned}$$

3) *The minimum distance of $\mathscr{C}(I)^{\perp}$ is equal to $2^{r_-(\mathscr{C}(I))+1}$*

C. Permutation Group

Applying an affine permutation to a monomial code yields a polynomial code but not necessarily a monomial code. Furthermore, polynomial codes and monomial codes may have a trivial permutation group. However by considering the subclass of decreasing monomial codes we obtain codes with a very large permutation group which contains the *lower triangular affine group*. Before giving its precise definition, we introduce some notation. Binary square matrices with m rows (and m columns) are denoted by $\mathrm{M}_m(\mathbb{F}_2)$. Let us recall that a bijective affine transformation over $\mathbb{F}_2^m$ can be represented by a pair $(\boldsymbol{A}, \boldsymbol{b})$ where $\boldsymbol{A}$ lies in the general linear group $\mathrm{GL}_m(\mathbb{F}_2)$ and $\boldsymbol{b}$ in $\mathbb{F}_2^m$. The action of $(\boldsymbol{A}, \boldsymbol{b})$ on a monomial g is denoted by $(\boldsymbol{A}, \boldsymbol{b}) \cdot g$. It basically consists in replacing each monomial x_i by a "new" monomial y_i defined by:

$$y_i = x_i + \sum_{j=0}^{m-1} a_{ij} x_j + b_i.$$

In the case of decreasing monomial codes, we are interested in a subclass of these transformations that are *lower triangular*. We recall that a matrix $\boldsymbol{A} = (a_{i,j})$ is lower triangular if $a_{i,j} = 0$ whenever $j > i$.

Definition 6. *The set of bijective affine transformations over $\mathbb{F}_2^m$ of the form $\boldsymbol{x} \mapsto \boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}$ where $\boldsymbol{A} \in \mathrm{GL}_m(\mathbb{F}_2)$ is a lower triangular binary matrix with $a_{i,i} = 1$ and $\boldsymbol{b} \in \mathbb{F}_2^m$ forms a group called the* lower triangular affine group $\mathrm{LTA}(m, 2)$.

Theorem 2. *The permutation group of a decreasing monomial code in m variables contains $\mathrm{LTA}(m, 2)$.*

Remark 1. *Although the permutation group of a Reed-Muller code is well-known, the question remains open for decreasing monomial codes.*

V. Minimum Weight Codewords

A natural object when dealing with group actions is the orbit of an element. We denote by $\mathcal{O}_g$ the orbit of a monomial g under the action of $\mathrm{LTA}(m, 2)$. When g is equal to the monomial x_i then its orbits is of the form $\left\{ x_i + \sum_{j=0}^{i-1} a_j x_j + b \mid a_j \text{ and } b \in \mathbb{F}_2 \right\}$. A consequence is that the cardinality of the orbit of x_i equals 2^{i+1}.

Definition 7. *For any $g \in \mathcal{M}_m$ let $\mathrm{LTA}(m,2)_g$ be the subgroup of $(\boldsymbol{A},\boldsymbol{b}) \in \mathrm{LTA}(m,2)$ such that:*

$$b_i = 0 \text{ if } i \notin \mathrm{ind}(g) \quad \text{and} \quad a_{ij} = \begin{cases} 0 \text{ if } i \notin \mathrm{ind}(g) \\ 0 \text{ if } j \in \mathrm{ind}(g). \end{cases}$$

We can remark that the action of $\mathrm{LTA}(m,2)_g$ on g consists in replacing each variable x_i of g by a "new" variable y_i defined by:

$$y_i = x_i + \sum_{j=0, j\notin \mathrm{ind} g}^{i-1} a_{ij}x_j + b_i.$$

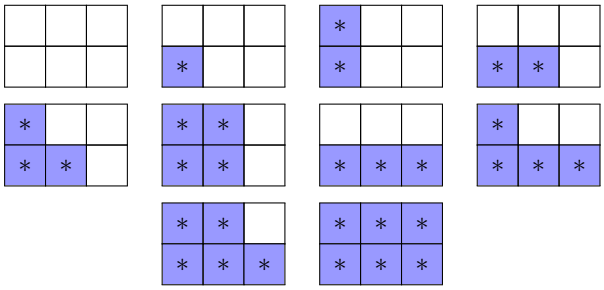
Proposition 4. *For any $g \in \mathcal{M}_m$ we have*

$$|\mathcal{O}_g| = |\mathrm{LTA}(m,2)_g|.$$

In order to give the cardinality of an orbit we use a well-known combinatorial object called the Ferrers diagram (or Young diagram).

Definition 8. *A* Ferrers diagram *is a finite collection of boxes arranged in left-justified rows, with the rows sizes weakly increasing.*

Figure 1. Ferrers diagrams in the 2×3 grid



We construct a bijection between Ferrers diagrams in the $d \times (m-d)$ grid and monomials of degree d in m variables. More precisely if $(\boldsymbol{A},\boldsymbol{b}) \in \mathrm{LTA}(m,2)_g$, then by definition of $\boldsymbol{A}$ the rows $i \notin \mathrm{ind}(g)$ and the columns $j \in \mathrm{ind}(g)$ contains only a 1 on the diagonal (and 0 elsewhere). If we remove from $\boldsymbol{A}$ the rows $i \notin \mathrm{ind}(g)$ and the columns $j \in \mathrm{ind}(g)$, we get a $d \times (m-d)$ matrix with possible non-zero coefficients exactly inside the boxes of the associated Ferrers diagram.

Proposition 5. *For any integers m, d with $1 \leqslant d \leqslant m$, there is a bijection between monomials in $\mathcal{M}_m$ of degree d and Ferrers diagrams in the $d \times (m-d)$ grid.*

We denote by λ_g the Ferrers diagram corresponding to g and $|\lambda_g|$ the size of a diagram, that is to say the number of $*$ in the diagram.

Exemple 1. *Let $m = 5$, $g = x_1x_4$ and take the matrix*

$$\boldsymbol{A} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ a_{10} & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ a_{40} & 0 & a_{42} & a_{43} & 1 \end{pmatrix}.$$

After deleting the rows corresponding to x_0, x_2, x_3 and the columns corresponding to x_1, x_4, we get $\begin{pmatrix} a_{10} & 0 & 0 \\ a_{40} & a_{42} & a_{43} \end{pmatrix}$ corresponding to the 8^{th} Ferrers diagram from Figure 1. We deduce that there are 2^4 different matrices $\boldsymbol{A}$ in $\mathrm{LTA}(m,2)_g$, and 2^2 different vectors $\boldsymbol{b}$ which gives $|\mathcal{O}_{x_1x_4}| = 2^6$.

Proposition 6. *The cardinality of the orbit of g under the action of $\mathrm{LTA}(m,2)$ is*

$$|\mathcal{O}_g| = 2^{\deg(g)+|\lambda_g|}$$

Characterizing the minimum weight codewords is often quite difficult and there are few families of codes where the structure of the minimum weight codewords is well known. In the case of decreasing monomial codes the subgroup $\mathrm{LTA}(m,2)$ gives enough information to understand the structure of the minimum weight codewords. We suppose that $\mathscr{C}(I)$ is a decreasing monomial code and we denote by $I_{r_+} = \{f \in I \mid \deg(f) = r_+\}$ the set of monomials in I of maximal degree. From Proposition 3, the set of minimum weight codewords is

$$W_{\min} = \{\boldsymbol{c} \in \mathscr{C}(I) \mid |\boldsymbol{c}| = 2^{m-r_+}\}.$$

Proposition 7. *Let $\mathscr{C}(I)$ be a decreasing monomial code.Then the number of minimum weight codewords in $\mathscr{C}(I)$ equals*

$$|W_{min}| = 2^{r_+} \sum_{g \in I_{r_+}} 2^{|\lambda_g|}.$$

Corollary 2. *The number of minimum weight codewords in $\mathscr{R}(r,m)$ equals*

$$W_{min}(\mathscr{R}(r,m)) = 2^r \binom{m}{r}_2$$

where $\binom{m}{r}_2 = \dfrac{(2^m-1)\dots(2^m-2^{r-1})}{(2^r-1)\dots(2^r-2^{r-1})}$ is the Gaussian binomial coefficient.

References

[1] E. Arıkan, "Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inform. Theory*, vol. 55, no. 7, pp. 3051–3073, 2009. [Online]. Available: http://dx.doi.org/10.1109/TIT.2009.2021379

[2] I. Dumer, "Soft-decision decoding of Reed-Muller codes: a simplified algorithm," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 954–963, 2006. [Online]. Available: http://dx.doi.org/10.1109/TIT.2005.864425

[3] I. Tal and A. Vardy, "How to construct polar codes," *IEEE Trans. Inform. Theory*, vol. 59, no. 10, pp. 6562–6582, 2013. [Online]. Available: http://dx.doi.org/10.1109/TIT.2013.2272694

[4] S. Kudekar, M. Mondelli, E. Sasoglu, and R. L. Urbanke, "Reed-Muller codes achieve capacity on the binary erasure channel under MAP decoding," 2015, arxiv:1505.05831[cs.IT]. [Online]. Available: http://arxiv.org/abs/1505.05831

[5] S. Kumar and H. D. Pfister, "Reed-Muller codes achieve capacity on erasure channels," 2015, arxiv:1505.05123[cs.IT]. [Online]. Available: http://arxiv.org/abs/1505.05123

[6] P. Charpin, "Codes cycliques étendus affines-invariants et antichaines d'un ensemble partiellement ordonne," *Discrete Math.*, vol. 80, no. 3, pp. 229–247, 1990. [Online]. Available: http://dx.doi.org/10.1016/0012-365X(90)90244-C

[7] R. Mori and T. Tanaka, "Performance and construction of polar codes on symmetric binary-input memoryless channels," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*. IEEE, 2009, pp. 1496–1500.

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 5th ed. Amsterdam: North–Holland, 1986.

[9] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, 'Ecole Polytechnique Fédérale de Lausanne (EPFL), Jul. 2009.